A Graduate Certificate in Information Systems Security Engineering

Presented to 3rd Annual UCDMO Conference

San Diego, CA

03 September 2009

Cynthia Irvine, Ph.D.
Department of Computer Science
Naval Postgraduate School

Problem

- Information Systems Security Engineering is needed for
  - NSA systems
  - DOD systems
  - Federal and private sector systems

- Information Systems Security Engineering is an art form
  - Learned from experienced mentors
  - Involves a steep and long learning curve
  - Some processes identified, but insufficient
  - Lack of repeatable, documented scientific methods
  - Not taught in universities

Mandate for Improvement (example)

- Cyber Security Act of 2009 (draft) Serves as an Example
  - Support programs to teach students how to
    1. design and build complex software-intensive systems that are secure and reliable when first deployed.
    2. test and verify that software, whether developed locally or obtained from a third party, is free of significant known security flaws.
    3. test and verify that software obtained from a third party correctly implements stated functionality, and only that functionality.
  - Support network security research in

    ‘‘(L) holistic system security that—

    ‘‘(i) addresses the building of secure systems from trusted and untrusted components;

    ‘‘(ii) proactively reduces vulnerabilities;

    ‘‘(iii) addresses insider threats; and

    ‘‘(iv) supports privacy in conjunction with improved security;

Question

- Can an ISSE educational program
  - Accelerate initial immersion of future ISSE professionals?
  - Provide a strong foundation for mastering the craft?
  - Begin to codify the scientific and engineering principals of information systems security engineering?
  - Become a source for establishing ISSE education at other colleges and universities?

More broadly, can the construction of secure information systems be transformed from a poorly understood art form, to a science, just as the construction of buildings and bridges has moved from the closed practices of the Medieval masons to a science (and art) based upon physics and engineering?

Origin of ISSE Education

- NSA interest in Cryptologic Computer Scientist education
- NPS response: a variety of course options
  - Information Systems Security Engineering sequence proposed
  - Other sequences included wide range computer science, e.g.
    - Vulnerability and Forensics, Text and Data Mining, etc.
- NSA and NPS held discussions about an ISSE program
  - NPS has
    - Experience in several high assurance efforts
    - Related research and development activities
    - Faculty and staff experienced and dedicated to teaching
    - Secure facilities to permit discussion of classified ISSE topics
    - Secure VTC for distance teaching
    - Cleared faculty

Evolution of ISSE Education

- Site visits by NSA personnel to NPS
  - Started in summer 2008
  - Subsequent visits to develop program
    - October 2008, January 2009, May 2009
  - Discussion of ISSE requirements
    - Technical
    - Team building
  - Brainstorming on important topics
    - Ensure adequate coverage in current classes
    - Discuss content of possible new courses
  - Identification of supporting materials and case studies
- Result
  - One new course
  - Two courses with major revisions

Two NPS Projects Inform ISSE

- Trusted Computing Exemplar
  - Investigate techniques for rapid development of high assurance systems
  - Develop exemplar
    - Least Privilege Separation Kernel
    - Trusted Path Extension Application
  - Evaluate – LPSK against SKPP, TPE against ST
  - Disseminate
- MYSEA Multilevel Testbed
  - Distributed architecture for high assurance MLS
  - Clients use popular commodity hardware and applications
  - Core elements of system high assurance for separation and controlled sharing of sensitive information
  - Support for legacy networks

ISSE Certificate

- Five courses for integrated approach
  - Network Security
  - Network Vulnerability Assessment and Risk Mitigation
  - Secure System Principles
  - Fundamentals of Information Systems Security Engineering
  - Applied Information Systems Security Engineering
- Two enrollment options for NSA participants
  - Graduate Certificate
    - Requires full admissions (BA or BS transcripts, etc.)
  - Professional Certificate
    - Participants just sign up
  - Grades and certificate completion on official NPS transcript
  - Courses applicable to graduate degree upon matriculation

Network Security

- Prerequisite for vulnerability assessment
- Concepts and technologies used to achieve integrity, confidentiality, and authenticity for information processed across networks. Topics include:
  - fundamentals of TCP/IP-based networking,
  - core network security principles,
  - traffic filtering types and methodology,
  - packet-level traffic analysis,
  - employment of cryptography,
  - tunneling/encapsulation,
  - Public Key Infrastructure (PKI),
  - remote authentication protocols, and
  - virtual private networks based on the IPSec, L2TP, and SSL protocols.

Network Vulnerability Assessment and Risk Mitigation

- Provides a basis for understanding potential vulnerabilities and their mitigation in networked systems by studying methods to:
  - obtain information about a remote network,
  - to possibly exploit or subvert systems residing on that network,
  - use techniques to mitigate risks to networked systems.
- Labs provide practical experience with current network attack and vulnerability assessment tools, as well as tools and methodologies for a systematic approach to reducing vulnerabilities. A final project that demonstrates skill and knowledge is required.

Secure System Principles

- Advanced presentation of key principles of a constructive approach to secure systems.
  - Includes operating systems and computer architecture review
  - Major topics include:
    - threat characterization and subversion;
    - policies and confinement;
    - fundamental abstractions, principles, and mechanisms, such as reduced complexity, hierarchical relationships, least privilege, hardware protection, resource management and virtualization, software security, secure system composition, mutual suspicion, synchronization, covert and side-channel analysis, secure metadata, secure operational states, usability, and life cycle assurance.
  - Current developments include advances in security hardware, components, and systems.

Fundamentals of Information Systems Security Engineering

- Fundamental principles and processes of information systems security engineering (ISSE).
- Stages of ISSE life cycle model: requirements definition, design, implementation, testing and deployment.
  - Processes explained in context of a Defense-in-Depth protection strategy, with an emphasis on the role of security requirements engineering (SRE) in the construction of a secure system.
  - Concepts and techniques to systematically elicit, derive and validate security requirements.
    - Practical application of techniques
    - Relationship between SRE and secure system design.
- Includes case studies and team project.

Applied Information Systems Security Engineering

- Key concepts and practices of information systems security engineering from a system life cycle perspective.
  - Core topics:
    - security architecture and design analysis,
    - system implementation assessment,
    - requirements and implementation traceability correspondence, security test and evaluation strategy,
    - certification and accreditation (C&A) requirements analysis,
    - risk management.
  - Reinforcement of principles, concepts and techniques
  - *Systems Thinking* approach to assess system security behaviors
  - Case studies & laboratory projects provide practical experience

Case studies

- Key element in several classes
  - Inform instructors
  - Enhance courses
  - Provide examples of how engineering is done correctly
  - Provide examples of mistakes and pitfalls

- Value of secure facilities and cleared faculty
  - At unclassified level, case studies must be sanitized
  - In classified spaces, free discussion of case study details is possible

Essential Elements

- Classes predicated on basic knowledge of security fundamentals
  - NPS has prepared CD-based study material based on existing information assurance course
    - Voice over by NPS faculty member provides details
    - On-line self assessments allow students to determine whether additional study is required

- Key element of all classes is practical experience
  - Paper exercises
  - Homework
  - Case studies
  - Laboratory work

Initial Pilot

- Began on 06 July 2009
  - Two academic quarters
  - Summer quarter
    - Network Security
    - Principles of Secure Systems
      - Lots of primary readings and analysis
    - Fundamentals of Information Systems Security Engineering
  - Fall quarter
    - Network Vulnerability Assessment and Risk Mitigation
      - Will entail considerable hands-on lab work
      - Students receive CNSSI 4012 (Senior System Manager) certification
    - Applied Information Systems Security Engineering
      - Half of the course devoted to case studies

Build NSA ISSE Community

- ISSE activities complex
  - No single person can *know it all*
  - Need to discuss challenges with others
  - Community that fosters
    - Non-judgmental, creative, exchange of ideas
- Hybrid delivery
  - Students at NPS for one week per quarter
  - Selected NSA mentors attend
  - Group discussion promoted
  - Group activities in evening
  - Classes and labs taken as a group rather than in isolation
- Classes, labs, and student activities in secure facility
    - Permits discussion of real problems rather than imaginary ones

Further ISSE Education Activities

- NPS CS uses specialization *tracks*
- Security Track highly popular
  - Has several *sub-tracks*
  - ISSE "sub-track" available to NPS students studying information assurance and cyber security
- NPS providing Masters in Computer Science to SPAWAR, Charleston
  - Distance learning
  - Using ISSE *sub-track*
  - Students currently taking core CS courses
  - ISSE courses start in Fall 2010

Other Educational Activities

- Pilot underway for separate NSA educational initiative
  - Two course sequence
    - Network Security
    - Advanced Vulnerability Assessment
  - Preceded by self study of information assurance basics
    - Voice over slides on CD and self assessments
  - Specialized text for advanced vulnerability assessment
    - The IDA Pro Book The Unofficial Guide to the World's Most Popular Disassembler by Chris Eagle
    - Taught by author

Identity Management Certificate

- Demonstrates NPS experience in certificate delivery
  - Provides overview of IDM concepts (light on math)
  - Four-course sequence taught in hybrid mode
    - Students at NPS for about 4 weeks during six-month program
      - NPS attendance significantly reduces attrition
    - Courses
      - Biometrics
      - Identity Management Infrastructure
      - Identity Management Policy
      - Identity Management Operations
    - Four cohorts per year
  - New: Data Fusion (now being taught as NPS resident course)
  - Information at: http://imep.nps.edu

Educational Model

- Certificates and non-resident degree programs
  - Requires non-NPS sponsor
  - Minimum class size: 15 students
  - Hybrid approach successful
    - Less student attrition
    - Community building
  - Lab requirements vary by course
    - Faculty and staff must manage lab software and hardware
    - Consistent configurations important
    - Options
      - NPS builds lab and delivers hardware and software to sponsor
      - Future – cloud model
        - » NPS houses lab
        - » Students use virtual network connection to access
        - » Maintenance and updates simplified

Summary

- Information Systems Security Engineering
  - More art than science
- Educational program intended to
  - Accelerate education of ISSE professionals
  - Find the science and engineering
- Pilot launched July 2009
  - Plan to learn from experience

ISSE team

- NSA: Kris Britton, Kevin Pelkey, Judy Wankrel
- NPS: Scott Cote, JD Fulp, Cynthia Irvine, Thuy Nguyen, Al Shaffer, Daniel Warren

Questions and Contacts

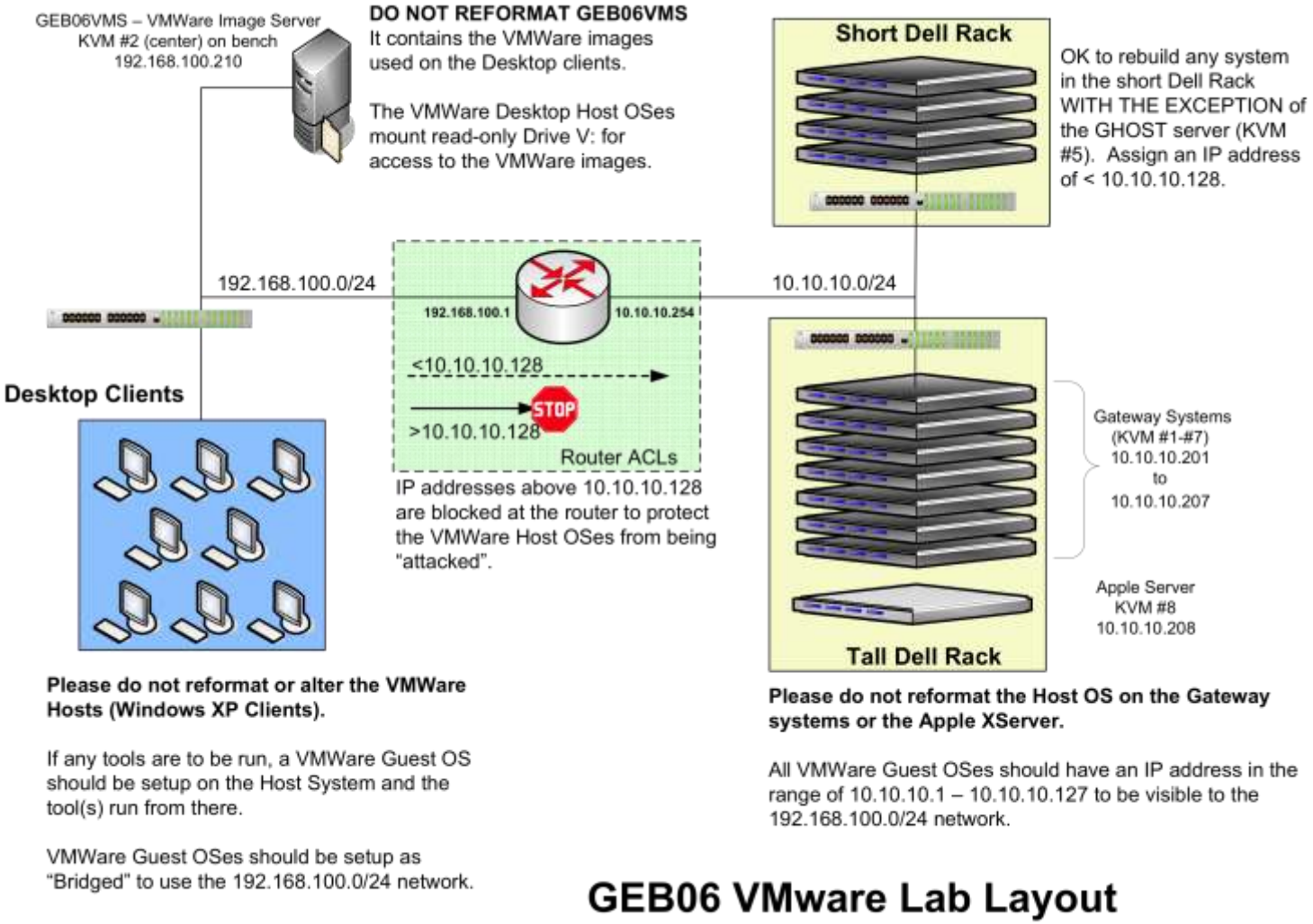
Cynthia Irvine, Ph.D.
irvine@nps.edu
831 656-2461

Center for Information Systems Security Studies and Research
Department of Computer Science
Naval Postgraduate School, Monterey, CA 93943

http://cisr.nps.edu

BACKUP SLIDES

Modeled on Existing NPS Lab



GEB06 VMware Lab Layout